

Reference 1

Japanese Patent Disclosure No. 2000-224156

(43)Date of Disclosure: August 11, 2000

(21)Japanese Patent Application No. 2000-12643

(22)Filing Date: January 21, 2000

(31)Convention Priority Number: 99101457.2

(32)Date of Priority: January 27, 1999

(33)Country of Priority: EPO

(71)Applicant: International Business Machines Corporation

(72)Inventor: Hermann Reto

The above Japanese Patent Disclosure No. 2000-224156 corresponds to European Patent Application No. 99101457.2.

The paragraphs in JP Publication to which the Examiner notices correspond to those paragraphs in EP publication as follows.

JP Publication

0010

0041

0051

EP publication

0011

0044

0054

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-224156

(P2000-224156A)

(43)公開日 平成12年8月11日(2000.8.11)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 M
H 0 4 L 12/28			1 0 9 S
		H 0 4 L 9/00	6 0 1 F

審査請求 有 請求項の数27 O L (全 11 頁) 最終頁に続く

(21)出願番号 特願2000-12643(P2000-12643)

(22)出願日 平成12年1月21日(2000.1.21)

(31)優先権主張番号 9 9 1 0 1 4 5 7 . 2

(32)優先日 平成11年1月27日(1999.1.27)

(33)優先権主張国 欧州特許庁 (E P)

(71)出願人 390009531

インターナショナル・ビジネス・マシー
ズ・コーポレーション

INTERNATIONAL BUSIN
ESS MACHINES CORPO
RATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(72)発明者 レト・ハーマン

スイス、シィ・エイチ-8863 プッティコ
ン、プールストラッセ 5

(74)代理人 100086243

弁理士 坂口 博 (外1名)

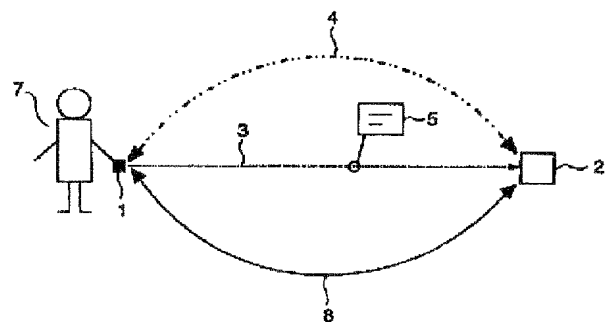
最終頁に続く

(54)【発明の名称】 ネットワーク化普及環境における情報交換のための方法、装置及び通信システム

(57)【要約】

【課題】 ネットワーク化普及環境における情報交換のための方法、装置及び通信システムを提供すること。

【解決手段】 認証された及び秘密のセッションが達成される。従って、第1の装置及び少なくとも第2のリモート装置が使用される。第1の装置及び第2のリモート装置間の単方向無線通信チャネルが始動され、第1の装置から第2のリモート装置への単方向無線通信チャネルを介して、シーケンスが送信され、第2のリモート装置に暗号化情報を提供する。前記暗号化情報を暗号化のために使用することにより、暗号化応答が無線同報媒体を介して第1の装置に送信される。



【特許請求の範囲】

【請求項 1】第 1 の装置と少なくとも第 2 のリモート装置との間の情報交換のための方法であって、前記第 1 の装置と前記第 2 のリモート装置との間の単方向無線通信チャネルを始動するステップと、前記単方向無線通信チャネルを介して、前記第 1 の装置から前記第 2 のリモート装置にシーケンスを送信し、前記第 2 のリモート装置に暗号化情報を提供するステップと、前記暗号化情報を暗号化のために使用し、無線同報媒体を介して、前記第 1 の装置に暗号化応答を送信するステップとを含む、方法。

【請求項 2】前記 2 つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、請求項 1 記載の方法。

【請求項 3】前記単方向無線通信チャネルが光チャネル、パーソナル・エリア・ネットワーク（PAN）・チャネル、有向無線周波チャネル、誘導性チャネル、または容量性チャネルである、請求項 1 記載の方法。

【請求項 4】前記単方向無線通信チャネルが有向チャネルである、請求項 1 または請求項 3 記載の方法。

【請求項 5】前記有向単方向無線通信チャネルが視線リンクである、請求項 4 記載の方法。

【請求項 6】前記第 1 の装置の初期送信機が、前記単方向無線通信チャネルが前記第 2 の装置に向けられるように配置される、請求項 1 記載の方法。

【請求項 7】前記無線同報媒体が光チャネル、音響チャネル、無線周波（RF）チャネル、ホーム RF チャネル、ブルートゥース・チャネル、またはパーソナル・エリア・ネットワーク（PAN）・チャネルである、請求項 1 または請求項 2 記載の方法。

【請求項 8】前記単方向無線通信チャネルが数メートルの通達距離を有し、前記無線同報媒体のチャネルが、前記単方向無線通信チャネルの前記通達距離と同一の、またはそれ以上の通達距離を有する、請求項 1 記載の方法。

【請求項 9】前記第 2 のリモート装置が前記シーケンスを受信する、請求項 1 記載の方法。

【請求項 10】前記第 2 のリモート装置が前記第 1 の装置からの前記シーケンスの受信を、光または音響信号により知らせる、請求項 1 記載の方法。

【請求項 11】前記第 2 のリモート装置が前記シーケンスを周期的に傾聴する、請求項 1 記載の方法。

【請求項 12】前記第 1 の装置がユーザに接続され、前記ユーザが前記第 2 のリモート装置に触れることにより、該ユーザの人体を介して前記単方向無線通信チャネルを始動する、請求項 1 記載の方法。

【請求項 13】前記 2 つの装置の 1 つが、少なくとも通信パラメータまたはセッション・キーを送信する、請求項 1 記載の方法。

【請求項 14】前記無線同報媒体を介する前記応答が、公開キー暗号化システムを含む、暗号化システムにより保護される、請求項 1 記載の方法。

【請求項 15】前記暗号化情報がパスワードまたは公開キーを含む、請求項 1 記載の方法。

【請求項 16】少なくとも 1 つのリモート装置との情報交換のための装置であって、単方向無線通信チャネルを介して、前記リモート装置にシーケンスを送信する初期送信機と、

前記リモート装置から無線同報媒体を介して暗号化情報を受信する受信機と、前記単方向無線通信チャネルを介して前記リモート装置に送信可能な暗号化情報を提供する暗号化システムとを含む、

前記受信機が前記無線同報媒体を介して、前記暗号化システムにより処理可能な暗号化情報を受信する、装置。

【請求項 17】少なくとも 1 つの装置との情報交換のための装置であって、

単方向無線通信チャネルを介して、前記装置からシーケンスを受信し、暗号化情報を獲得する初期受信機と、前記暗号化情報を処理する暗号化システムと、暗号化情報を無線同報媒体を介して前記装置に送信する送信機とを含む、装置。

【請求項 18】情報を符号化及び復号する暗号化システムを有する第 1 の装置及び第 2 の装置を含む、情報の交換のための通信システムであって、

前記第 1 の装置が、単方向無線通信チャネルを介して、前記第 2 の装置にシーケンスを送信し、前記第 2 の装置に暗号化情報を提供する初期送信機と、

無線同報媒体を介する前記第 1 及び第 2 の装置間の暗号化通信のための第 1 のトランシーバとを含み、

前記第 2 の装置が、前記単方向無線通信チャネルを介して、前記第 1 の装置から前記シーケンスを受信し、前記暗号化情報を獲得する初期受信機と、

前記無線同報媒体を介する前記第 1 及び第 2 の装置間の暗号化通信のための第 2 のトランシーバとを含む、通信システム。

【請求項 19】前記無線同報媒体を介して暗号化情報を送信可能な送信機を含む、請求項 16 記載の装置。

【請求項 20】前記初期送信機が前記シーケンスを前記単方向無線通信チャネルを介して、数メートルの通達距離内で送信する、請求項 16 記載の装置。

【請求項 21】前記無線同報媒体が光チャネル、音響チャネル、無線周波（RF）チャネル、ホーム RF チャネル、ブルートゥース・チャネル、またはパーソナル・エリア・ネットワーク（PAN）・チャネルである、請求項 16 または請求項 17 記載の装置。

【請求項 22】前記無線同報媒体が前記単方向無線通信

チャンネルの通達距離と同一の、またはそれ以上の通達距離を有する、請求項 16 または請求項 17 記載の装置。

【請求項 23】LED などの光装置またはラウドスピーカなどの音響装置により、前記シーケンスの受信を知らせるシグナル装置を含む、請求項 17 記載の装置。

【請求項 24】前記初期受信機が前記シーケンスを周期的に傾聴する、請求項 17 記載の装置。

【請求項 25】前記 2 つの装置の 1 つが通信パラメータ及びセッション・キーを送信できる、請求項 18 記載の通信システム。

【請求項 26】前記 2 つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、請求項 18 記載の通信システム。

【請求項 27】前記第 1 の装置の前記初期送信機が、前記単方向無線通信チャンネルが視線リンクにより前記第 2 の装置に向けられるように配置される、請求項 18 記載の通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク化普及環境における情報交換のための方法、装置及び通信システムに関し、特に、装置が認証されたセッションまたは秘密セッションに参加することを可能にする初期技法に関する。

【0002】

【従来の技術】コンピュータは、劇的に小型化され、携帯可能となった大規模で珍しい孤立した装置である。パーソナル・コンピュータ及び周辺装置は、机上に載置可能なように十分に小さくなった。より小型のものにラップトップ・コンピュータ及びノートブック・コンピュータがある。配送トラックなどの乗り物に搭載可能なように、十分に小さなコンピュータ端末が存在する。更に小型のものにハンドヘルド端末があり、これは一般にその携帯性により、ユーザが片手で端末を持ち運び、もう一方の手でそれを操作することができる。ケーブルまたはファイバによる前記装置の物理接続はケーブルの長さ制限や、コンピュータ上のポート数の制限、従って接続可能な周辺装置の数の制限、或いはハードワイヤード装置の厄介な再構成などのために構造的制限などの欠点を有する。コンピュータ上の限られたポート数が、実際には周辺装置の数を制限しない幾つかの周辺インタフェース・システムが存在する。ユニバーサル・シリアル・バス(USB)及びIEEE1394(ファイヤワイヤ)は、単一ポート上で非常に多数の装置をサポートできる周辺バス・システムの例である。イーサネットは、ケーブルが共用媒体として使用される通信システムの例である(他の例にはトークン・リング、FDDI(ファイバ分散データ・インタフェース)、及びDQDB(分散キュー・デュアル・バス)がある)。

【0003】装置が小型化するほど、固定の物理接続を

無線アドホック接続(例えば人体ネットワーク、無線周波接続、または赤外線接続)により置換することが重要となる。なぜなら、コンピュータ端末、周辺装置、及び他の装置をケーブルまたはファイバにより物理的に接続することは、ユニットを小型化することにより得られる効果を多大に低減するからである。装置が移動され、ある領域から出たり入ったりする場合、アドホック接続が要求される。用語“アドホック(ad-hoc)”は頻繁なネットワーク再構成の必要性を指す。

10 【0004】ローカル・エリア通信は、パーソナル・ローカル・エリア・ネットワークと呼ばれるものに急速に発展しつつある。これはローカル・ピアまたはサブシステム間の通信のためのネットワークである。これらの種類のネットワークを、ここではローカル・ネットワークと呼ぶことにする。無線通信はこうしたローカル・ネットワークでは、特に重要である。こうしたローカル・ネットワークのピアまたはサブシステム間の通信を目的とする、既知の異なる無線通信アプローチが存在する。

【0005】ローカル・ネットワークの典型的な例は、20 パーソナル・エリア・ネットワーク(PAN)であり、これはマサチューセッツ工科大学(MIT)メディア研究所の 2 つの研究グループ間の業績により誕生した。人体の自然塩分は、人体を電流の優れた導体にする。PAN 技術はこの導電性を利用する。PAN 技術はごく僅かな電流を用いて、ユーザの識別及び他の情報がある人から別の人に、或いは自動車、公衆電話、自動預金支払機(ATM)などの様々な日常物にさえも伝送する。情報は、厚いクレジットカード・サイズの PAN 送信機及び受信機内に配置されるマイクロプロセッサを介して転送される。次にデジタル・データが、微小の外部電界を介して送信または受信される。小信号が人体の自然塩分により伝導され、気付かれることなく、情報を人体を通じて伝達する。低周波及び低電力の信号は個人に符号化される情報が人体を超えて伝達されず、人体と接触するある物または誰かによってのみ受信されることを保証する。情報が現在伝送されるスピードは、2400 ボー・モデムに等価である。理論的には、この方法により 400000(すなわち 400k)ビット/秒が伝達され得る。PAN は固定のケーブル接続などを要求しないアドホック人体ネットワークの典型的な例である。

40 【0006】PAN 技術はビジネス、医療、小売り、及び個人分野においてさえ、潜在的なアプリケーションを有する。例えばビジネス仲間は握手を交わしながら電子名刺を交換する。企業の機密装置は、自動的にユーザをコンピュータ・システムにログオン及びログオフし、地下鉄通勤者は回転式改札を通過することにより、乗車運賃を支払う。PAN 技術により、人々は自身の医療ファイルのデジタル・バージョンを持ち運び、それにより緊急医師による即時アクセスが可能となる。或いは、呼び出しカード番号が自動的に財布から公衆電話に送信され

得る。また、ATM及び自動車はそれらの所有者が近くとき、即時所有者を識別することができる。別のアプリケーション分野は、売買に参加するために立場で素早く且つ確実なログオン及びログオフを要求する商人に当てはまる。CDプレーヤ、テレビ及びトースタなどの家電機器でさえも、PAN技術の使用により、個人の嗜好及び味覚を識別し、それらに適応することができる。PANネットワークは通常ポイント間通信であり、そこでは人体が同報通信媒体として作用する。

【0007】GTE社は、セルラ電話、ページャ、及び10 ハンドヘルド・パーソナル・コンピュータ(PC)などの移動装置をターゲットとする、お互いの対話にとって好適な短距離無線周波(RF)技術を開発した。GTE社の技術は暫定的に、ボディLAN(ローカル・エリア・ネットワーク)と命名される。ボディLANの元々の開発は、様々な装置に接続された配線付きベストを介するものであった(これがボディLANの名前に由来する)。これが数年前にRF接続へと進歩した。

【0008】ゼロックス社は、PARC TABと呼ばれる10 ハンドヘルド・コンピュータ装置を開発した。PARC TABは携帯式であるが、既知のロケーションを有するベース・ステーションを介して、オフィス・ワークステーションに接続される。PARC TABベース・ステーションは建物のあちこちに配置され、固定の配線式ネットワークに配線される。PARC TABシステムは、建物レイアウトの所定の知識、及び様々なベース・ステーションの識別子を用いることにより、最も強いベース・ステーション信号により、自身がどこにあるかを決定する。PARC TABシステムは、PARC TAB携帯装置が常にネットワーク構造基盤に接続されて10 いるものと仮定する。各PARC TAB装置のロケーションは、常にシステム・ソフトウェアに知れている。ベース・ステーションは領域を確立し、電源に接続される。PARC TAB通信システムはスター型トポロジを有する。

【0009】異種のPC装置間のデータ通信を標準化するために、エリクソン、IBM、インテル、ノキア(Nokia)及び東芝を含む幾つかの会社が、固定の携帯用移動装置間の無線RFベースの接続のための世界標準を作成するために、ブルートゥース(Bluetooth)・コンソーシアムを確立した。多くの他の採用会社が存在する。提案された規格は、物理層からアプリケーション層までのアーキテクチャ及びプロトコル仕様を含む。この技術は例えば、ユーザがオフィスに入るとき、移動装置内に保持されるアプリケーション情報を、固定のデスクトップ・コンピュータ内に保持される同様の情報と自動的に同期させる解決策を可能にする。ワイヤレス短距離無線を介して、継ぎ目の無い音声及びデータ伝送を可能にすることにより、ブルートゥース技術はケーブルを必要とすることなく、ユーザが様々な装置を容易に且つ迅速に50

接続することを可能にし、移動コンピュータ、移動電話及び他の移動装置の通信能力を拡大する。ブルートゥース動作環境はまだ完全に定義されていないが、IrDA(赤外線データ・アソシエーション)仕様及び拡張赤外線(AIr)仕様との類似点があるものと期待される。多分ブルートゥースに盛り込まれるであろう他の態様は、IEEE規格802.11、及び欧州電気通信規格協会(ETSI)により公布されたHIPERLANに由来するであろう。

【0010】ブルートゥース無線技術は、固定のネットワーク構造基盤から離れて存在する接続装置の、小規模で専用のアドホックグループを形成する機構を提供する。ブルートゥースは、マスタ・ユニットと、同一のネットワーク・セグメント内のスレーブ・ユニットとを区別し、前者はそのクロック及びホッピング・シーケンスが、他の全ての装置を同期するために使用される装置である。換言すると、ブルートゥース・アプローチは集中化される。照会ベースの発見技法が、未知のアドレスを有するブルートゥース装置を見いだすために使用される。照会はまた、レジストリ・サーバにおいて集中化される。故障の中央ポイントが存在することは、こうした集中型アプローチの欠点である。こうしたシステムの別の欠点は、分散技法よりも多くのオーバヘッドが要求されることである。こうしたシステムの主問題は、単一のレジストリ・サーバを突き止めることにあり、それが消えた場合にどうすべきかにある。無作為の2つの装置が互いに遭遇する場合、それらは最初にお互いの存在を認識し、次にどちらがレジストリ・サーバかを決定し、続いてそれらの通信の作業に取りかからねばならない。オーバヘッドの増加を生じるのは、リーダのこの頻繁な選択及び再選択である。別の方法は、ユーザが常にある装置を身につけて持ち運んでいるものと期待し、それを常にリーダとすることである。しかしながら、これは常に現実的な選択とは限らない。

【0011】IrDAは、赤外線技術の品質及び相互運用性を保証する赤外線規格及び仕様を提供することを目的とする、世界中の150社以上の協会である。IrDA-Aは、1mの距離のデータ転送用に設計された赤外線データ伝送規格であり、115kビット/秒乃至4Mビット/秒、または近い将来16Mビット/秒をサポートする予定である。広範囲のハードウェア及びソフトウェア・プラットフォームがサポートされる。IrDAデータは、相互運用可能な汎用双方向コードレス赤外線光伝送データ・ポートのための規格を定義し、高速短距離、視線、ポイント間コードレス・データ転送に適している。IrDAデータ・プロトコルは、強制プロトコルと任意プロトコルのセットを含む。しかしながら、元来の仕様は幾つかの欠点を示し、ある時点に1対の装置だけが同一の赤外線空間において通信可能のように、データ通信を制限する。ヒューレット・パッカード及びIB

Mの両者間の協力により、次世代の赤外線データ通信システムを定義する拡張赤外線(AIr)と呼ばれる別の仕様が開発された。AIrは、室内におけるマルチポイント対マルチポイント接続のために提案される。距離及びデータ速度は可変であり、8mの距離において250kビット/秒から、4mの距離において4Mビット/秒の範囲に及ぶ。これは複数の周辺装置へのコードレス接続、及び会議室共同アプリケーションのために設計された。IrDAに関する詳細は、IrDAウェブ・サイト”<http://www.irda.org>”で見い出される。

【0012】ホームRF(共用無線アクセス・プロトコル(SWAP)にもとづく)は、装置を接続するために使用され得る動作環境の別の例である。ホームRFワーキング・グループは、家庭内または周辺のPCと、家電製品との間の無線デジタル通信のための開かれた業界仕様を確立することにより、広範囲に渡る相互運用可能な消費者製品のための基礎を提供するために結成された。ワーキング・グループには、パーソナル・コンピュータ、家電製品、周辺装置、通信、ソフトウェア、及び半導体業界からの主要企業が含まれ、SWAPと呼ばれる家庭における無線通信のための仕様を開発中である。ホームRF SWAPシステムは、音声及びデータ・トラフィックの両方を伝送し、公衆交換電話網(PSTN)及びインターネットと相互運用するように設計される。すなわち、これは2400MHz帯で動作し、デジタル周波ホッピング・スプレッド・スペクトル無線を使用する。SWAP技術は既存のコードレス電話(DECT)及び無線LAN技術の拡張から導出され、ホーム・コードレス・サービスの新たなクラスを可能にする。これは対話音声及び他の時間に厳格なサービスの転送を提供する時分割多重アクセス(TDMA)サービスと、高速パケット・データの転送のためのキャリア検知多重アクセス/衝突回避(CDMA/CA)サービスの両方をサポートする。SWAPシステムはアドホックネットワークとして、または接続ポイントの制御に従う管理ネットワークとして動作する。アドホックネットワークでは、データ通信だけがサポートされ、全てのステーションが等しく、ネットワークの制御がステーション間で分散される。対話音声などの時間に厳格な通信では、PSTNへのゲートウェイを提供する接続ポイントが、システムを調整するために要求される。ステーションはCSMA/CAを使用し、接続ポイント及び他のステーションと通信する。ホームRFに関する詳細は、ホーム無線周波ワーキング・グループのウェブ・サイト”<http://www.homerf.org>”で見い出される。SWAP仕様1.0が参考として本明細書に組み込まれる。

【0013】伝送される情報は、意図された受信者に制限され、誰にでも好適な訳ではない。秘密の及び認証された通信を想定すると、暗号化方式が役に立ち、有用である。暗号化システムは、メッセージが”秘密(secure

e)”となるように、メッセージを送信者から受信者に媒体を介して送信するためのシステムである。すなわち、意図された受信者だけがメッセージを復元することができる。暗号化システムは平文とも呼ばれるメッセージを、暗号文と呼ばれる暗号化形式に変換する。暗号化は、暗号キーを用いてメッセージを操作または変換することにより達成される。受信者は暗号文を平文に変換することにより、メッセージを解読する。これは暗号キーを用いて、操作または変換プロセスを逆処理することにより実行される。こうした暗号化伝送は、送信者及び受信者だけが暗号キーの知識を有する限り、安全である。過去に、公開キー暗号化システムなどの幾つかの暗号化システムが提案されている。公開キー暗号化システムでは、私用キーが常に算術的に公開キーにリンクされる。例えば、既知の公開キー暗号化システムは、Diffie-Hellmanキー規約、RSA方式、またはElGamal方式である。適応選択された暗号文攻撃に対して多分安全であろう順応性の無い公開キー暗号化システムが、R. Cramer及びV. Shoupにより提案されている。

【0014】

【発明が解決しようとする課題】本発明の目的は、ネットワーク化普及環境における装置間の情報交換のための技法を提供することである。

【0015】本発明の別の目的は、通信ピアを識別する技法を提供することである。

【0016】更に本発明の別の目的は、少なくとも2つの装置間で、認証された通信セッションを確立するための技法を提供することである。

【0017】更に本発明の別の目的は、少なくとも2つの装置間で、プライバシーを保証する秘密の通信セッションのための技法を提供することである。

【0018】

【課題を解決するための手段】本発明は一般にローカル・ネットワークに関し、特に、認証されたまたは秘密の通信セッションのセットアップに関する。局所的に分散された装置がセッションを確立し、情報を交換することを可能にする初期技法が提案される。こうしたセッションは、機能ユニットまたは装置間のデータ通信の目的で使用される。ここで用語”セッション”は、接続の確立、保守、及び解除の間に発生する全ての活動を意味する。本発明によれば、ネットワーク化普及コンピュータ環境において、少なくとも2つの装置がセッションに参加する。

【0019】基本概念は、ユーザが着用するパーソナル・アシスタントなどの個人用装置である第1の装置と、ユーザの近くにあるサーバ装置などの第2の装置との間で、認証されたセッション、すなわちユーザにより許可されたセッションを確立したいユーザが、有向短距離通信リンクを使用し、通信セッションを開始する。従って、第1の装置が暗号化情報及び通信パラメータをター

10

20

30

40

50

ゲット装置に伝送する。ターゲット装置すなわち第2の装置は、受信情報及びパラメータを使用し、発信装置すなわち第1の装置への無線同報接続を確立する。本発明の別の部分は、秘密セッションを保証するキーの実装、及び個人用装置とサーバ装置間の通信が発生する時間フレームの制御である。

【0020】ユーザの個人用装置とサーバ装置、例えば銀行端末との間で認証されたセッションを確立するために、ユーザは個人用装置によりサーバ装置を指し示すか、少なくともこの方向を指定し、例えば赤外線チャンネルなどの単方向無線通信チャンネルを介して、パスワード、公開キー、セッション・キー、識別パラメータ、及び通信パラメータなどを含むシーケンスまたは初期シーケンスを伝送する。シーケンスの受信後、サーバ装置は無線同報媒体を介して、暗号化情報を返送することにより応答する。暗号化情報は、個人用装置によってのみ解読され、使用され得る。この応答は、無線同報媒体を介する以後の通信のためのサーバ装置からの情報、キー、セッション・キー、及び通信パラメータを含み得る。個人用装置が暗号化情報を受信する。

【0021】無線同報媒体を介する秘密セッションのために、キーが交換される。従って、無線同報媒体を介する暗号化通信が発生する。

【0022】どの装置が通信パラメータまたはセッション・キーを送信するかは、問題でない。

【0023】それにも関わらず、個人用装置をサーバ装置の方向に配置する要求は、通信パートナーを選択するための非常に直感的な方法を許容する。人々は子供の時から物を指し示すことになれている。更に、指し示す方法は、明示的に通信ターゲットを選択する利点を有する。すなわち、例えばPANリンクでは、ユーザは実際に通信ターゲットに触れる必要があり、レーザ・リンクでは、通信パートナーが視覚的に選択され得る。

【0024】2つの装置が同一の無線同報媒体を共用し、ローカル・ネットワークの一部の場合、たとえ個人用装置を有するユーザが別の部屋または階に歩いていくことにより、自分の位置を変えても、開始セッションが継続され得る利点がある。これは個人用装置が大きなファイルをダウンロードしたり、サーバ装置と長い時間通信する場合に役立つ。無線同報媒体としては、赤外線（IR）チャンネルまたは無線周波（RF）チャンネル、特にIrDAチャンネル、ホームRFチャンネル、ブルートゥース・チャンネル、パーソナル・エリア・ネットワーク（PAN）・チャンネル、音響チャンネル、またはユーザに広範囲のアクションを保証する他のチャンネルが使用され得る。

【0025】通信セッションを開始し、機密情報を含み得る初期シーケンスを伝送するために、単方向無線通信チャンネルがターゲット装置だけが初期シーケンスを受信することを保証する。これは特に、有向チャンネルが視線

リンクとして使用され得る場合に有利である。なぜなら、他の当事者が立ち聞きし、初期シーケンスを受信できないからである。こうしたチャンネルは、赤外線またはレーザ・チャンネルなどの光チャンネル、パーソナル・エリア・ネットワーク（PAN）・チャンネル、有向無線周波（RF）チャンネル、誘導チャンネル、容量チャンネル、または短距離有向通信リンクに好適な他のチャンネルである。

【0026】サーバ装置が個人用装置からのシーケンスの受信を知らせる場合、ユーザはフィードバックを獲得し、サーバ装置が追加の通信のために準備完了状態であることを知る利点がある。これはランプ、LEDまたはラウドスピーカにより与えられる光信号または音響信号により示される。

【0027】サーバ装置が周期的に個人装置からのシーケンスに傾聴するとき、送信されるシーケンスが即時処理され得る利点がある。

【0028】個人装置が例えばPANによりユーザに接続される場合、通信をセットアップすることは非常に単純である。なぜなら、ユーザは直感的にサーバ装置に触れ、自身の人体を介して有向無線通信チャンネルを開始するからである。認証されたセッションをセットアップするために、追加のカードや他の物は必要とされない。

【0029】無線同報媒体を介する応答及び追加の通信が、暗号化システムの使用により保護される場合、交換情報が完全に隠され、別の誰かにより暴露され得ない利点がある。好適なシステムは、公開キーが1度交換される公開キー暗号化システムである。

【0030】更に本発明の別の利点は、無線単方向リンクの場合、個人装置とサーバ装置との直接的な接触が必要でないことである。例えば、キャッシュカード、スマートカード、または個人装置内の任意の他のカード、或いは個人装置自体に、例えば電子メール、データまたは金額などの情報が、相対距離からロードまたはアップロードされ得る。カードは装置または読取り装置内に配置される必要はなく、このことは読出しエラーを回避し、PINコードを余分に形成し、時間の節約に役立つ。

【0031】秘密セッションがサーバ装置のすぐそばまたは正面で開始し、遠い距離において安全に継続され得る。サーバ装置はこれらの装置が有用な至る所、例えば銀行、オフィス、倉庫、ショッピング・センタ及び屋外などに設置される。これはユーザに行動の大きな独立性及び自由をもたらす。例えば、サーバ装置がコンサートの広告のすぐ近くに配置される。このコンサートのチケットは、ユーザが駅のプラットフォームで電車を待っている間に、コンサートの広告を見るときに購入され、代金を支払われる。チケットはカード上または個人用装置上に電子的に記憶されるか、コンサートの入口においてアップロードされ得る。ユーザはチケット売場で行列になって待つ必要はなく、チケットを買い忘れることもない。

【0032】

【発明の実施の形態】本発明の目的上、用語“ネットワーク化普及コンピュータ環境（networked pervasive computing environment）”は、無線ネットワーク技術を通じて通信する携帯用情報装置及び固定情報装置の両方の環境として定義される。こうした環境内での装置間の通信は、近距離を基本とする。これらの装置の始動通信範囲は小さい。従って、装置が近い距離にあるときだけ、セッションが開始され得る。更に、通信関係の確立は、アドホック的性質（ad-hoc nature）を有する。これはすなわち、物理層上での通信が、任意の2つの装置が近い距離にあるとき、常に発生し得ることを意味する。こうした装置のユーザは情報の流れを制御する必要があり、これは特に、クレジットカード詳細や権限などの機密情報に当てはまる。種々の問題は、機構について述べるセッション制御である。

【0033】本発明の状況では、ローカル・ネットワークが、互いの相互通信範囲内の少なくとも2つの装置からなるネットワークとして定義される。こうしたローカル・ネットワーク内では、装置は配線式ネットワークの必要無しに、互いに通信する。ローカル・ネットワークは固定ネットワークとの接続のために、アクセス・ポイントを有する必要がない。ローカル・ネットワークは他のネットワークから完全に分離されるか、無線装置に配線式ネットワークとの接続を提供する1つ以上のアクセス・ポイントを含み得る。

【0034】本発明に従いローカル・ネットワークを構成する特定の範囲は、実際の実装詳細に依存する。一般に、ローカル・ネットワークは、数平方メートル乃至数百平方メートルの通達範囲を有するものとして述べられる。特定の状況下では、通信範囲は更に広がる。

【0035】本発明のネットワーク技術は、倉庫、製造フロア、オフィス、立合場、自宅、自動車及びトラック、航空機、及び屋外などで使用され得る。

【0036】用語“装置”は、ローカル・ネットワークのメンバである任意の種類の装置を意味する。こうした装置の例には、ラップトップ・コンピュータ、ワークパッド、ノートパッド、パーソナル・デジタル・アシスタント（PDA）、ノートブック・コンピュータ及び他の着用可能なコンピュータ、デスクトップ・コンピュータ、コンピュータ端末、ネットワーク・コンピュータ、インターネット端末及び他のコンピュータ・システム、セットトップ・ボックス、キャッシュ・レジスタ、バーコード・スキャナ、ポイント・オブ・セールス（POS）端末、キオスク・システム、セルラ電話、ページャ、腕時計、デジタル時計、バッジ、スマートカード、及び他のハンドヘルド及び組み込み装置などがある。他の装置には、ヘッドセット、ヒューマン・インタフェース装置（HID）準拠の周辺装置、データ及び音声アクセス・ポイント、カメラ、プリンタ、ファックス・マシン、キ

ーボード、ジョイスティック、台所器具、道具、発煙及び発火検出器などのセンサ、及び事実上あらゆる他のデジタル装置が含まれる。

【0037】本発明と共に使用され得る着用可能なコンピュータの他の例には、“スマート・ウォレット”・コンピュータ、宝石類、または衣類など、コンピュータ風のハードウェアを装備された身の回り品がある。“スマート・ウォレット”・コンピュータに加え、着用可能なコンピュータの多数の他の変形が存在する。“ベルト”・コンピュータは、ユーザが動き回る間に、文書をサーフし（surf）、書き留め、編集することを可能にする変形である。更に別の例は、小学生用のパーソナル・デジタル・アシスタントに匹敵する子供のコンピュータである。子供のコンピュータは宿題を保持し、計算を実行し、子供が宿題を管理することを手助けする。それは他の子供のコンピュータとインタフェースし、共同作業を容易にし、また先生のコンピュータにアクセスして、宿題またはフィードバックをダウンロードする。任意の着用可能または携帯可能な装置、オフィス・ツールまたは装置、家庭用ツールまたは装置、乗り物用システム、或いは公衆用システム（自動販売機、チケット自動販売機、自動預金支払機など）が、本発明の状況において使用され得る。

【0038】ネットワーク・トポロジ：本技法は、ポイント間及びポイント・マルチポイント間接続を有するローカル・ネットワークで使用され得る。幾つかのネットワーク・セグメント（グループ）が確立され、アドホックに一緒にリンクされ得る。ネットワーク・トポロジは、本発明のテーマよりも低レベルである。ネットワーク・トポロジの態様は、必要な程度だけ示される。本発明はネットワーク・トポロジとは無関係であり、同報を可能にする任意の種類のネットワーク・トポロジ上使用され得る。

【0039】ネットワーク技術：本技法は、RF、IRまたは他の光技術、人体ネットワーク（PANなど）などの、任意の無線通信技術に関連して使用され得る。

【0040】以下では、本技法の典型的な実装（第1の実施例）について、図1及び図2に関連して述べることにする。

【0041】図1では、ユーザの手の中にある第1の装置1と、ユーザの近くにある第2の装置2との間の情報の交換のために、認証されたセッション8をセットアップしたいユーザ7を示す簡単な概略図である。そのために、ユーザ7は第1の装置1を物理的に第2の装置2の方向に向け、接続を開始する。第1の装置1は暗号化情報を有するシーケンス5を、単方向無線通信チャネル3を介してターゲット装置すなわち第2の装置2に送信する。単方向無線通信チャネル3がセキュリティを保証する有向視線リンクとして、例えば赤外線チャネルとして確立されることが有利である。なぜなら、別の誰もリン

クを傾聴できないからである。第2の装置2は、プリンタまたは別の人間の装置であり、パスワード、キー、通信パラメータ、または識別パラメータを含むシーケンス5を受信し、受信情報を用いて第1の装置に対して、所望の認証されたセッション8をセットアップする。無線同報媒体4がその目的のために使用される。

【0042】図2は、図1のより詳細な構成を示す。第1の装置1は、初期送信機10、第1のトランシーバ11、及び第1の暗号化システム15を含む。これらの全てのユニットは第1の処理ユニット16に接続され、後者は簡略化のために図示されていない更に別のユニットに接続される。第1のトランシーバ11は、第1の同報受信機12及び第1の同報送信機13を有する。他方、第2の装置2は、初期受信機20、第2のトランシーバ21、及び第2の暗号化システム25を含む。第2の装置2の全てのユニットは第2の処理ユニット26に接続され、後者は簡略化のために図示されていない、データ処理のための更に別のユニット、またはネットワークにさえも接続される。第2のトランシーバ21は、第2の同報送信機22及び第2の同報受信機23を有する。更に、第2の装置2はシグナル装置30を示し、これはここではLEDである。このLED30は中央処理ユニット26に接続される。2つの暗号化システム15、25のタスクは、情報を暗号化及び解読し、交換される情報を隠し、保護することである。

【0043】認証を提供するために、本技法は公開キー技法を使用する。これはすなわち、第1の当事者が、私用キー及び暗号化アルゴリズムを用いて公開キーを生成し、この公開キーを第2の当事者に送信するか、公開キーを他の当事者が使用可能にする。次に、例えば第2の当事者が、受信された公開キーを用いて情報を暗号化する。暗号化された情報が、例えば無線周波(RF)チャネルなどの無線同報媒体など、不確かな媒体またはチャネルを介して返送される。しかしながら、第1の当事者だけが私用キーを用いて、この情報を解読できる。

【0044】本発明に従う初期技法は、次のように作用する。図2では簡略化のため示されていないユーザ7が、初期送信機10を用いて、第1の装置1から単方向無線通信チャネル3を介してシーケンス5を送信する。ここではシーケンス5は開始トークン T_{init} を含み、単方向無線通信チャネル3は、第2の装置2への有向IRチャネルである。開始トークン T_{init} は、第1の装置1の公開キー K_{pub}^P 、及びランダムに選択されたアドホックデータ $nonce_P$ を含む。単方向無線通信チャネル3を介して、開始トークン T_{init} を伝送することにより、目標の第2の装置2だけがそれを受信し、応答することができる。第2の装置2が初期受信機20においてシーケンス5を受信し、第2の処理ユニット26がシーケンス5を通知され、受け渡される場合、LED30が第1の中央処理ユニット16によりトリガされ、ユーザ

7に第2の装置2が準備完了状態で、通信セッションを開始できることを知らせる。セッションはいつでもユーザにより制御され、これはすなわち、ユーザが即時セッションを停止できることを意味する。通常、第2の装置2は、受信される開始トークン T_{init} に反応して、第2の同報送信機22から無線同報媒体4を介して、公開キー・トークン T_{pub} を応答6として第1の装置1に返送する。ここでは無線同報媒体4は無線周波(RF)である。第2の暗号化システム25により生成される公開キー・トークン T_{pub} は、第2の装置2の公開キー

K_{pub}^S 、及び受信されたアドホックデータ $nonce_P$ の連結を含む。公開キー・トークン T_{pub} は、開始トークン T_{init} 内で受信された第1の装置の公開キー K_{pub}^P を用いて暗号化される。最後に、第1の装置1は第1の主受信機12により応答を受信し、第1の処理ユニット16及び第1の暗号化システム15により、この応答を処理し、第1の同報送信機13により、通信パラメータ・トークン T_{com} を含む通信シーケンス9を返送する。この通信シーケンス9もまた、無線同報媒体4を介して伝送され、第2の装置2の第2の同報受信機23により受信される。通信パラメータ・トークン T_{com} は、第2の装置2の受信公開キー K_{pub}^S により暗号化される。

【0045】交換されるトークンは、算術的に次のように表すことができる。

$$\text{【数1】 } T_{init} = K_{pub}^P || nonce_P$$

$$\text{【数2】 } T_{pub} = [K_{pub}^S || nonce_P] K_{pub}^P$$

$$\text{【数3】 } T_{com} = [Com] K_{pub}^S$$

【0046】第1の暗号化システム15は、開始トークン T_{init} 及び通信パラメータ・トークン T_{com} を提供し、第2の暗号化システムは公開キー・トークン T_{pub} を提供する。

【0047】第1の装置と第2の装置間の続く通信は、第1のトランシーバ11及び第2のトランシーバ21を用い、無線同報媒体4を介して発生する。それにより、第1の装置1により指定された通信パラメータが使用される。

【0048】セッションの認証について、前述の第1の実施例で述べた。しかしながら、クレジットカード情報などの機密情報を交換するために、認証だけでは十分でない。第1の装置と第2の装置間の保護された専用通信リンクが必要とされる。従って、第2の実施例は、通信パラメータ・トークン T_{com} 内に、第1の装置1の第1の暗号化システム14により生成される暗号化セッション・キー K_{sess}^P を含むことにより達成される。両方の装置間の続く各通信は、このセッション・キー K_{sess}^P を用いて暗号化される。

【0049】別の実施例が、第1及び第2の実施例に関連して、以下で述べられる。一般に、個人用装置である第1の装置1と、サーバ装置である第2の装置との間の対話は、特定のタイミング状況において発生する。サー

バ装置2が開始トークン T_{init} を何度も再使用することを阻止するために、満期日 $T_{D_{init}}$ が開始トークン T_{init} に付加される。両者はシーケンス5内で伝送される。個人用装置1は、開始トークン T_{init} に付加された満期日 $T_{D_{init}}$ がまだ過ぎていなければ、公開キー・トークン T_{pub} に応答する。満期日 $T_{D_{init}}$ は個人用装置1の時間の観念に関連する。

【0050】更に別の実施例は、前述の実施例の変形である。満期日開始トークン $T_{D_{init}}$ 同様、満期日 $T_{D_{sess}}$ が、個人装置または第1の装置1により生成されるセッション・キー K_{sess} に付加され、無線同報媒体4を介して伝送される。満期日 $T_{D_{sess}}$ の実装は、応答装置2に応答の定義期限を提供する。この期限が過ぎると、伝送は要求されず、セッションは停止される。これは携帯装置の電力を節約し、セキュリティを提供するために役立つ。

【0051】開始トークン T_{init} を有するシーケンス5を、無線通信チャンネル3を介してサーバ装置2に転送することは、ユーザ7の明示的な制御に従うべきである。単方向無線通信チャンネル3として使用される技術に応じて、この問題は異なって扱われる。単方向無線通信チャンネル3（以下、（短距離）単方向チャンネル）を介する通信は、デフォルト指定により無効にされる。単方向チャンネル3がレーザ・ポインタの光リンクの場合、次の2段階プロシージャが問題を解決する。すなわち、（1）ユーザ7が第1のボタンを押下して、レーザを活動化し、レーザビームが目標対象物の表面に当たるとき、レーザビーム・スポットのビジュアル制御により、レーザを所望の方向に向け、（2）ユーザ7がレーザビームが対象物に当たっていると判断するとき、ユーザは第2のボタンを押下し、実際に開始トークン T_{init} を有するシーケンス5をターゲット装置2に送信する。単方向チャンネル3がPAN技術にもとづく場合、次の2段階プロシージャが問題を解決する。すなわち、（1）ユーザ7が第1のボタンを押下することにより、単方向チャンネル3を使用可能にする。一旦活動化されると、単方向チャンネル3はある限定時間 δt の間活動化され、その間に、ユーザ7はPAN可能面に触れることにより、シーケンス5を有向チャンネル3を介して伝送する機会を有する。（2）ユーザ7はPAN可能面に触れることにより、実際にシーケンス5を単方向チャンネル3を介して伝送する。 δT の経過後、単方向チャンネル3を介する通信が即時無効化され、追加の偶発的な情報交換を阻止する。

【0052】活動化プロシージャの拡張は、ユーザが個人用装置の第1のボタンを繰り返し押下することにより、 δT を長引かせることができる場合である。

【0053】更に、個人用装置は、汎用無線通信チャンネル3を即時無効化するための類似の手段を提供すべきである。

【0054】任意の開示実施例が、ここで示された1つ

のまたは複数の他の実施例と組み合わせられ得る。これは実施例の1つ以上のフィーチャについても可能である。

【0055】まとめとして、本発明の構成に関して以下の事項を開示する。

【0056】（1）第1の装置と少なくとも第2のリモート装置との間の情報交換のための方法であって、前記第1の装置と前記第2のリモート装置との間の単方向無線通信チャンネルを始動するステップと、前記単方向無線通信チャンネルを介して、前記第1の装置から前記第2のリモート装置にシーケンスを送信し、前記第2のリモート装置に暗号化情報を提供するステップと、前記暗号化情報を暗号化のために使用し、無線同報媒体を介して、前記第1の装置に暗号化応答を送信するステップとを含む、方法。

（2）前記2つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、前記（1）記載の方法。

（3）前記単方向無線通信チャンネルが光チャンネル、パーソナル・エリア・ネットワーク（PAN）・チャンネル、有向無線周波チャンネル、誘導性チャンネル、または容量性チャンネルである、前記（1）記載の方法。

（4）前記単方向無線通信チャンネルが有向チャンネルである、前記（1）または（3）記載の方法。

（5）前記有向単方向無線通信チャンネルが視線リンクである、前記（4）記載の方法。

（6）前記第1の装置の初期送信機が、前記単方向無線通信チャンネルが前記第2の装置に向けられるように配置される、前記（1）記載の方法。

（7）前記無線同報媒体が光チャンネル、音響チャンネル、無線周波（RF）チャンネル、ホームRFチャンネル、ブルートゥース・チャンネル、またはパーソナル・エリア・ネットワーク（PAN）・チャンネルである、前記（1）または（2）記載の方法。

（8）前記単方向無線通信チャンネルが数メートルの通達距離を有し、前記無線同報媒体のチャンネルが、前記単方向無線通信チャンネルの前記通達距離と同一の、またはそれ以上の通達距離を有する、前記（1）記載の方法。

（9）前記第2のリモート装置が前記シーケンスを受信する、前記（1）記載の方法。

（10）前記第2のリモート装置が前記第1の装置からの前記シーケンスの受信を、光または音響信号により知らせる、前記（1）記載の方法。

（11）前記第2のリモート装置が前記シーケンスを周期的に傾聴する、前記（1）記載の方法。

（12）前記第1の装置がユーザに接続され、前記ユーザが前記第2のリモート装置に触れることにより、該ユーザの人体を介して前記単方向無線通信チャンネルを始動する、前記（1）記載の方法。

（13）前記2つの装置の1つが、少なくとも通信パラメータまたはセッション・キーを送信する、前記（1）

記載の方法。

(14) 前記無線同報媒体を介する前記応答が、公開キー暗号化システムを含む、暗号化システムにより保護される、前記(1)記載の方法。

(15) 前記暗号化情報がパスワードまたは公開キーを含む、前記(1)記載の方法。

(16) 少なくとも1つのリモート装置との情報交換のための装置であって、単方向無線通信チャンネルを介して、前記リモート装置にシーケンスを送信する初期送信機と、前記リモート装置から無線同報媒体を介して暗号化情報を受信する受信機と、前記単方向無線通信チャンネルを介して前記リモート装置に送信可能な暗号化情報を提供する暗号化システムとを含み、前記受信機が前記無線同報媒体を介して、前記暗号化システムにより処理可能な暗号化情報を受信する、装置。

(17) 少なくとも1つの装置との情報交換のための装置であって、単方向無線通信チャンネルを介して、前記装置からシーケンスを受信し、暗号化情報を獲得する初期受信機と、前記暗号化情報を処理する暗号化システムと、暗号化情報を無線同報媒体を介して前記装置に送信する送信機とを含む、装置。

(18) 情報を符号化及び復号する暗号化システムを有する第1の装置及び第2の装置を含む、情報の交換のための通信システムであって、前記第1の装置が、単方向無線通信チャンネルを介して、前記第2の装置にシーケンスを送信し、前記第2の装置に暗号化情報を提供する初期送信機と、無線同報媒体を介する前記第1及び第2の装置間の暗号化通信のための第1のトランシーバとを含み、前記第2の装置が、前記単方向無線通信チャンネルを介して、前記第1の装置から前記シーケンスを受信し、前記暗号化情報を獲得する初期受信機と、前記無線同報媒体を介する前記第1及び第2の装置間の暗号化通信のための第2のトランシーバとを含む、通信システム。

(19) 前記無線同報媒体を介して暗号化情報を送信可能な送信機を含む、前記(16)記載の装置。

(20) 前記初期送信機が前記シーケンスを前記単方向無線通信チャンネルを介して、数メートルの通達距離内で送信する、前記(16)記載の装置。

(21) 前記無線同報媒体が光チャンネル、音響チャンネル、無線周波(RF)チャンネル、ホームRFチャンネル、ブルートゥース・チャンネル、またはパーソナル・エリア・ネットワーク(PAN)・チャンネルである、前記(1

6)または(17)記載の装置。

(22) 前記無線同報媒体が前記単方向無線通信チャンネルの通達距離と同一の、またはそれ以上の通達距離を有する、前記(16)または(17)記載の装置。

(23) LEDなどの光装置またはラウドスピーカなどの音響装置により、前記シーケンスの受信を知らせるシグナル装置を含む、前記(17)記載の装置。

(24) 前記初期受信機が前記シーケンスを周期的に傾聴する、前記(17)記載の装置。

(25) 前記2つの装置の1つが通信パラメータ及びセッション・キーを送信できる、前記(18)記載の通信システム。

(26) 前記2つの装置が前記無線同報媒体を共用し、ローカル・ネットワークの一部である、前記(18)記載の通信システム。

(27) 前記第1の装置の前記初期送信機が、前記単方向無線通信チャンネルが視線リンクにより前記第2の装置に向けられるように配置される、前記(18)記載の通信システム。

【図面の簡単な説明】

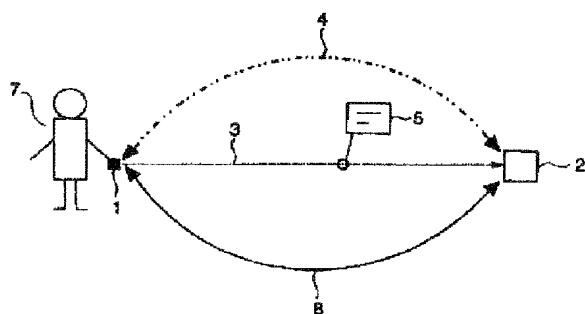
【図1】ユーザが自身の個人用装置とリモート・サーバ装置との間で、認証されたセッションを確立したい場合に、本発明に従うアプリケーションの概略図である。

【図2】図1の詳細概略図である。

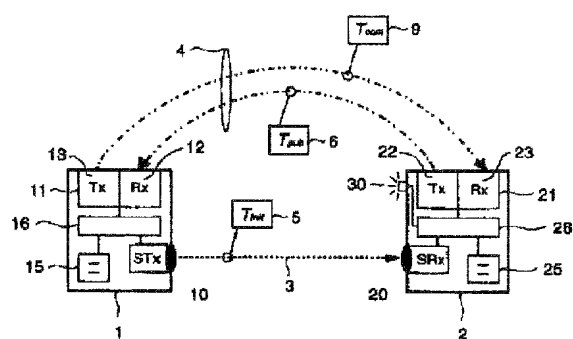
【符号の説明】

- 1 第1の装置
- 2 第2の装置
- 3 単方向無線通信チャンネル
- 4 無線同報媒体
- 5、9 通信シーケンス
- 7 ユーザ
- 8 認証されたセッション
- 9 応答
- 10 初期送信機
- 11、21 トランシーバ
- 12、23 同報受信機
- 13、22 同報送信機
- 15、25 暗号化システム
- 16、26 処理ユニット
- 20 初期受信機
- 30 LED

【図1】



【図2】



フロントページの続き

(51)Int.Cl.

識別記号

F I

H 0 4 L 11/00

リモート (参考)

3 1 0 B

(72)発明者 ダーク・フセマン
 スイス、シィ・エイチー8134 アドリスウ
 イル、クレプスバックウェグ 4